学校编码：10384　　分类号_____密级_____
学号：23020101153005　　UDC_____

厦门大学

硕士学位论文

一种基于身份的椭圆曲线数字签名方案及其在门禁系统中的应用

An Identity-Based Signature Agreement on Elliptic Curve and the Use in Access Control System

傅希鸣

指导教师：郑建德　教授

专业名称：计算机技术
论文提交日期：2013 年 5 月
论文答辩日期：2013 年 5 月
学位授予日期：2013 年　月

答辩委员会主席：_____
评　阅　人：_____

2013 年　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

2013 年 5 月 31 日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

2013年5月31日

摘要

门禁控制系统是安全技术防范领域的重要组成部分，采用现代电子与信息技术，对建筑物内外正常的出入通道进行管理，控制人员出入。随着门禁控制系统的广泛应用，门禁控制系统的安全性研究一直是人们的关注焦点，安全性、身份识别、系统安全管理等问题是该领域研究的热点，为防控区域提供安全的保障是门禁控制系统的灵魂及核心。可以说，安全性主宰着门禁系统的发展方向。

本文设计了一套新型门禁系统，该系统采用一种新型的数字签名算法来保证系统的安全性。数字签名是手写签名的数字化形式，能够在数据传输过程中提供一系列的安全服务，如认证性、完整性与抗抵赖性等等。然而传统的数字签名体制涉及到数字证书的管理问题，需要花费高昂的成本。为解决这样的问题，本文提出了一种椭圆曲线下基于身份的数字签名算法，该算法与一般的基于身份数字签名算法一样可以有效避免了复杂的证书托管问题。具体来说，本文的主要工作如下：

1、本文首先对经典的基于身份的数字签名算法进行了分析，并提出了一种新型的在椭圆曲线密码体制下基于身份的数字签名方案，该签名方案具有密钥长度短、运算规模小并且无需对认证实体与密钥进行复杂管理等优点，适合于移动设备、嵌入式系统等处理能力较弱的设备。

2、将该数字签名算法结合到手机令牌身份认证方案中，该方案以手机作为令牌，采用“挑战-应答”认证模式，将时间戳作为挑战，对挑战作数字签名成为应答，以二维码图像的方式传递应答码。

3、本文最后设计了一套新型的智能安全门禁系统并将手机令牌认证方案应用到其中，该系统采用嵌入式设备作为认证端，手机令牌作为客户端，密钥颁发机构运行于独立的服务器上，认证时采用离线认证的方式，无需密钥颁发机构的参与，从而构成了一套同时具备高安全性、高便捷性和高实用性的新型门禁系统。

关键字：椭圆曲线；基于身份的数字签名；手机令牌；二维码；门禁系统

Abstract

The access control system is an important part in the field of security technology, which makes use of modern electronics and information technology, to manage the access of the building. With the widely application of access control systems, the research on security has always been a hot topic in this field, such as security, identification and system safety management. It is core and vital to provide security for the prevention and control area. It is security that dominates the direction of development of the access control system.

In this paper, we design a set of new access control system, the system uses a new kind of digital signature algorithm to guarantee the security of system. Digital signature is an important branch of cryptography in the modern information security research category. Digital signature is a digital form of handwritten signature, which could provide a series of security services during the process of data transmission, such as authentication, integrity and non-repudiation. However, the cost on management of digital certificates would be too high in traditional digital signature system. In this paper, a digital signature algorithm based on identity provides a good solution to this problem. The main idea is to blend user’s information to the corresponding key, thus avoiding the complex certificate escrow problem. Specifically, this paper's main work is as follows:

1, In the first part of the paper, the digital signature algorism based on identity is analyzed, and a new kind of Identity-Based Signature Agreement on Elliptic Curve is introduced. The length of key is shorter, the computation scale is small and there is no need for complex entity and key management in the new agreement. Therefore, the new scheme is especially applicable to equipment with weak processing power, such as mobile devices and embedded systems.

2, Then, we combine this digital signature to the mobile token authentication scheme, regard mobile phone as a token, adopts the model of "the challenge - response" certification (where timestamp as a challenge and related digital signature as response), and transfer response code through QR code image.

3, Finally, a new type of intelligent entrance guard system is designed, where phone token authentication scheme is applied, embedded devices is regarded as authenticator and mobile phone token as the client, the key issue institutions runs on

another server to realize off-line authentication, thus an access control system with high security, high availability and high practicability is realized.

Key Words: Elliptic Curve; Identity-Based Digital Signature; Mobile Phone Token; QR Code; Access Control System

目 录

Table of Contents

第一章 绪论

1.1 课题背景

门禁控制系统是安全技术防范领域的重要组成部分，采用现代电子与信息技术，对建筑物内外正常的出入通道进行管理，控制人员出入，或控制人员在建筑物内及其相关区域的行动，实施放行、拒绝、记录和报警等操作。随着门禁控制系统的广泛应用，门禁控制系统的安全性研究一直是人们的关注焦点，卡的安全性、身份识别、系统安全管理等问题是该领域研究的热点，为防控区域提供安全的保障是门禁控制系统的灵魂及核心。可以说安全性主宰着门禁系统的发展方向。如图 1.1 所示，门禁控制系统一般由门禁管理系统、控制执行机构和目标识别子系统三个部分组成。

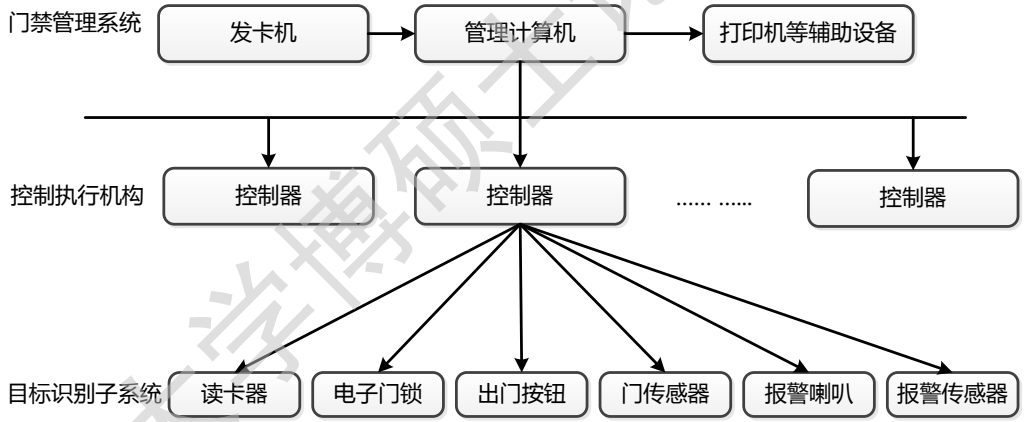

图 1.1 门禁控制系统结构图

门禁系统中的身份识别安全性是研究的重点，由门禁系统的三部分共同完成，身份识别是通过提出出入门禁人员的身份信息，将其传递给管理与控制部分，管理与控制部分再与所有的资料对比，确认同一性，核实目标的身份，以便进行各种控制处理，一般有卡识别和生物特征识别两种方式。

卡识别是目前门禁系统中应用最为广泛的识别方式之一，一般使用 IC 卡作为识别信息数据载体，但是由于卡上存有出入门禁的身份鉴别信息，往往是非法入侵者攻击的目标。

影响 IC 卡及门禁系统安全的主要方式有一下几种：

(1) 使用用户丢失或被窃的 IC 卡，冒充合法用户进入门禁控制系统的防控区域。

(2) 非法使用伪造卡或空白卡复制数据，进入门禁控制系统的防控区域。

(3) 使用系统外的 IC 卡读写设备，对合法卡上的数据进行修改，非法进入门禁系统防控区域。

(4) 在 IC 卡读写操作中，对读卡器与 IC 卡通信时的交换信息流进行截获，修改，已达到非法入侵的目的。

基于以上种种不安全因素，对于卡识别的门禁系统，需要采取相应的防护措施来保证门禁系统的安全性。

生物特征识别是利用人体固有的生理特征或行为特征来进行个人身份鉴定的识别技术，主要包括：指纹识别、人脸识别、视网膜识别、掌形识别等，从识别的角度来说，这种识别方式安全性很高，且不需要携带多余的卡片。但是该识别方式成本较高，识别率易受环境因素影响，对环境及使用者的要求很高。因此目前没有广泛的推广该技术在门禁上的应用。

鉴于目前广泛使用的门禁控制系统所存在的一些缺陷，使用新型的技术应用于门禁系统，是提高门禁系统安全性的研究方向。

1.2 研究现状

门禁系统是在传统门锁的基础上发展而来的，后者是机械装置，但是在出入人很多的地方，例如办公室，酒店等，钥匙的管理不便。随着电子技术的发展，这一问题得到了解决，出现了电子磁卡锁，电子密码锁等电子门禁系统，该系统提高了人们对出入口的管理程度。又随着电子芯片的高度集成化和生物识别技术的发展，智能门禁系统得以出现。以下是门禁系统的发展过程[1]：

第一代门禁：键盘输入密码方式——会有因忘记密码而被拒之门外。

第二代门禁：接触卡式门禁系统，例如：

(1)磁码卡，是把瓷质贴在朔料卡片上制成。磁卡可改写，应用方便。缺点是易消磁，易磨损。

(2)铁码卡，是用特殊的金属线排列编码，采用金属磁烧的原理制成，不易被复制。铁码卡有效防磁，防水，防尘，是一种安全性较高的卡，缺点是卡片不小心被消磁或弄脏，进入人员将被拒之门外。